Current
Policy No. 230

The Challenge of Terrorism: the 1980s

September 25, 1980

United States Department of State
Bureau of Public Affairs
Washington, D.C.

NEWARK PUBLIC LIBRARY
NOV 19 1980
U.S. GOVT. PUBS.
DEPOSITORY 376

Following is an address by Ambassador Anthony C. E. Quainton, Director of the Office for Combatting Terrorism, before the American Society for Industrial Security in Miami, September 25, 1980.

Violence abounds in our world. Governments and corporations are equally affected. The statistics for 1979 were horrendous: worldwide, 293 major incidents including 46 assassinations, 20 kidnappings, 13 hostage-barricade situations, not to mention bombings and armed attack; 77 of these terrorist incidents directly involved U.S. citizens or property. High on the list came the kidnapping and murder of our Ambassador to Afghanistan in February 1979, the seizure of our Embassy in Iran in November, and the killing of eight of our citizens in violent attacks in Turkey throughout the year.

The story for 1980 is even more alarming. In the first 8 months alone, there have been 500 incidents, of which 101 have involved Americans. One American Ambassador was taken hostage in Bogota and held for 61 days; another in Beirut narrowly escaped assassination a month ago. Americans have been kidnapped and held for ransom in Guatemala and Colombia. Overall, 58 countries have been the target of at least one attack. Even the Soviet Union, which many have thought immune, has had to face over 30 terrorist attacks, putting it second in the listing of countries most frequently targeted. The United States, alas, remains in first place.

Major Incidents

In 1979 and 1980, the private sector has been particularly hard hit. Let me cite the major incidents in 1979 of which I am aware which were directed against your corporations:

Jan. 3	General manager of Texaco in Colombia, killed, having been held hostage since the previous May.
Feb. 13	Cairo Sheraton bombed, 17 people injured.
Feb. 19	Pan American office in Izmir, Turkey, bombed.
Apr. 19	Explosives detonated at the Ford Motor Co. showroom in Valencia.
Apr. 23	Subsidiary of Babcock and Wilcox bombed in Dusseldorf.
May 20	IBM office in San Salvador, strafed.
June 15	Nicaraguan manager of National Cash Register, kidnapped in El Salvador.
June 20	American Airlines jet, hijacked to Ireland by a Serbian nationalist.
July 24	Offices of the Wells Fargo Bank in Istanbul, bombed.
Aug. 14	Factory of Apex Textile Co. seized in El Salvador, its American general manager held for 9 days.
Sept. 21	Two American executives of Beckman Instruments kidnapped in El Salvador.
Oct. 26/28	Citicorp's deputy manager shot to death; Bank of America office bombed—both in El Salvador.

S1.71/4:

Nov. 26	Armenian terrorists bomb Western Airlines and TWA in Madrid.
Dec. 3	Morgan Guarantee Trust in Frankfurt, bombed.
Dec. 5	W. R. Grace fertilizer plant in Trinidad, bombed.
Dec. 14	Three Boeing contract employees killed in Istanbul.
Dec. 23	TWA bombed in Rome.
Dec. 25	Citibank and ITT bombed in El Salvador.

In 1980 there has been no respite. In Trinidad, a Texaco refinery was bombed, as were TWA offices in Madrid. A Texaco regional vice president was abducted in Honduras. A similar attempt was made against a Colgate Palmolive executive in Cali, Colombia. And in the last month, a series of bombings have damaged banks and other American corporation premises in Manila. Finally, the month of August enters into the Guiness book of terrorist records as the month with the most hijackings, all of American aircraft.

I have cited for you only some of the more dramatic incidents which have directly affected U.S. interests. I have not mentioned, for example, the Corsican terrorists' attempt to blow up an oil refinery near Marseilles or the successful attack againt South Africa's major synthetic fuels manufacturing plant. These two incidents have a particular significance since they represent attacks on highly sensitive facilities rather than the more traditional symbolic attacks on airline offices and banks.

In the last year we have also seen a new phenomenon—systematic assassinations by states of their political enemies abroad. Assassinations have succeeded in 24 countries with 23 different groups involved. The assassinations have included Libyans and Iraqis in Europe, Syrians in Jordan, Iranians in the United States and, most recently, the killing of ex-President Somoza in Paraguay. The international community is faced with a growing lawlessness, a diminishing respect for international law, a continuing erosion of the basic principles of diplomatic intercourse. There is no reason to suppose that these attacks will stop. We must anticipate increasing numbers of violent acts as the 1980s advance.

What we did not see in the 1970s was any significant escalation of terrorist tactics. To be sure, in the last 2 years there have been more casualties than ever before. But the terrorists continue to kill with relatively unsophisticated weapons: homemade bombs, automatic weapons, and rocket-propelled grenades. We have seen no evidence that terrorists are about to turn to esoteric weapons (nuclear, chemical, or biological), recent novels such as the *Fifth Horseman* notwithstanding.

There are, however, some indications that we may see a change to new and more significant targets. If so, the private sector will be directly affected. It is evident to most of us that in modern society there are numerous vulnerabilities: computers, power generation and transmission systems, tankers, off-shore oil facilities. Many of these are only lightly protected. Security for these installations will require the most careful attention in the years ahead and the closest possible cooperation between government and industry. The cost will be high.

I have attended several conferences in the last 6 months at which these issues have been discussed and at which industry and government representatives have begun to examine together ways in which we can address the next generation of problems. At this point, we cannot predict with any certainty which facilities or which industries are most likely to be attacked or threatened. However, given the high stakes and the potential costs of being unprepared, we must be sure that the best minds available are doing the contingency planning which is needed.

Strategy for Combatting Terrorism

Before returning to the question of what needs to be done in the future, let me review for you what we have already achieved. In the last 5 years, we have developed a strategy for combatting terrorism and other forms of low-level violence which has five elements: intelligence, physical security, contingency planning, crisis management, and international cooperation. None of these is new; all have been significantly improved and upgraded in recent years. In the crucible of events our competence has been refined. We have learned a number of lessons which should stand us in good stead as we approach the 21st century.

Intelligence. In some ways the most important lesson is that intelligence in the broadest sense is critical. Ten years ago we knew little about terrorist groups, their leaders, or their *modus operandi*. This situation has dramatically changed, notwithstanding self-imposed restraints on some kinds of intelligence activity. We now do have computer data bases which enable us rapidly to factor information about terrorist groups into our crisis management system.

Most significantly we have information about terrorist plans. Almost every week somewhere in the world we are informed of a specific threat against one of our diplomats or embassies or against a private corporation, airline, or executive. Without exception, this information is passed to our Embassies through diplomatic channels or, in the case of the private sector, through the State Department's Office of Security to the corporation concerned. Intelligence is worthless if it is not used. It is a highly perishable commodity. Although we must be concerned to protect sensitive sources and methods, I can assure you whenever we are aware of information which affects the security of your companies or your executives, you will be the first to know.

Physical Security. Unfortunately, intelligence provides only a partial answer. We will not have forewarning of all terrorist attacks. The problems of penetrating small, highly dedicated terrorist cells are enormous. The resources available are limited. We must therefore take other measures to deter attacks, the most obvious of which is physical security. I do not pretend to be an expert in this field, and certainly with so much talent and expertise in the audience, I am hesitant to offer any guidance. Nonetheless, I am convinced that security does pay off. Our Ambassador in Beirut was saved in an assassination attempt last month because he was in a specially protected vehicle and had armed and trained professional security officers with him. Our Embassy and Ambassador's residence in Bogota were not attacked this spring because the M-19 concluded that the protective systems in place were too difficult to breach. They chose the Dominican Republic Embassy instead. Only once, in fact, in Kuala Lumpur in 1976, has an American Embassy been taken over by a terrorist group. Everywhere else terrorists have been successfully deterred.

Unfortunately, the systems created to deter the entry of terrorists were insufficient to deal with the mob violence which we saw in Pakistan, Iran, and Libya in the last year. We are now embarked on a major upgrading of our Embassy security at a cost of over $40 million to improve perimeter controls and to develop the concept of internal safehavens. We must give our personnel abroad the protection which they need in a world of growing violence and in which governments may be unable or unwilling to come to our assistance promptly. No task has a higher priority for our security experts in the Department.

In the last decade we have also made notable progress in deterring hijackings. With almost 20,000 weapons seized at American airports since 1974, we know that the systems works. Only one plane in all that time has been hijacked in the United States with a weapon taken through screening. Now we are faced with a new weapon—flammable liquid. Improved screening methods will have to be devised. The Federal Aviation Administration (FAA) is already actively engaged in seeking a solution to this new threat.

We all know that security is only as good as its weakest link. We, as you, must be alert to any weaknesses so that we can enhance our protective systems and thereby diminish the vulnerability of those we are called on to protect. But weaknesses there will always be, and we must assume that terrorists occasionally will succeed in taking hostages or in carrying out some other violent act. When terrorists succeed, we must be prepared with adequate contingency plans and a crisis management structure that insures that all appropriate resources are rapidly deployed toward the resolution of the incident.

Contingency Planning and Crisis Management. We have given high priority to contingency planning. Every American Embassy and consulate is required to have plans to cover bomb threats, internal defense, hijackings, and hostage incidents. Every Federal Bureau of Investigation (FBI) field office in the United States has plans for handling terrorist incidents in collaboration with appropriate local law enforcement agencies. The Federal Government has a national response plan for nuclear emergencies, including terrorist attacks. There now exists a credibility assessment system for all kinds of nuclear and other esoteric threats. Within hours through this system the Federal Government can obtain a succinct and technically sound appraisal of any threat received. We are looking, as a priority, at ways to improve our contingency plans for handling incidents in the maritime environment. The counterterrorist joint task force which the Department of Defense is creating as a result of Admiral Holloway's report will provide yet another level of contingency preparedness. The purpose of all of these plans and preparations is to make certain that we have ready and clearly defined lines of command and control and the necessary supporting resources, including communications, which we will need to manage a crisis.

Plans only provide a framework within which crisis managers can act. They do not provide policy guidelines nor insure the harmonious working of a system which ultimately depends on the personal relations which exist among representatives of various agencies and jurisdictions. In recent years we have worked to build experienced teams of area and intelligence experts, behavioral scientists, security professionals, public relations officers. They are used to working together. They understand the basic policy framework in which they must act. They have training in the basic principles of hostage negotiation and crisis management. When there are major policy issues to be addressed in the course of an incident, they are taken promptly to the special coordination committee (SCC) of the National Security Council. The SCC is the policy-level group to which the working group on terrorism and its executive committee report for guidance. Similarly, the lead agency responsible for managing an incident (the FBI/Justice domestically, the State Department abroad, the FAA in the case of hijackings) would also get its guidance from the SCC.

As part of our preparation for future terrorist attacks, we have given high priority to the training of all employees of all Federal Government agencies serving abroad. At the Foreign Service Institute in Washington we offer a course on terrorism and coping with violence which provides an introduction to such subjects as surveillance recognition, travel precautions and countering vehicular kidnapping, recognition of and defenses against letter and parcel bombs, residential security, protection against local crime, preparedness for riots and demonstrations, preparation for family separations and evacuations, and hostage survival. We are now paying particular attention to the needs of families, for our experience has been that they must be part of any emergency planning system. Spouses and other adult family members attend all our counterterrorist and security training courses.

Increasingly, in our contingency planning and crisis management we have come to recognize that no one agency has all the answers. Crisis management is a team effort in which many agencies and many layers of state and local government are involved. In more and more incidents, the private sector is an essential element of this partnership. In hijackings, the airline concerned is always a part of the government crisis network sharing in the decisions and listening and contributing to the analysis of the evolving situation. Similar structures may be needed in the future if we are faced with other kinds of terrorist attacks or hostage incidents involving corporate assets and personnel.

Because of the need for close cooperation, we must face squarely the fact that we do not always agree. In some terrorist incidents, the government and private industry may have conflicting interests, priorities, and policies. For example, industry usually pays ransom, the government does not. Yet both are concerned for the lives at stake in the immediate situation and for the possibility that others will be at risk in the future. Both should be aware of the political radicalization which may result from giving in to terrorist demands. To the extent that ransom fuels the coffers of revolutionary groups, long-term government and corporate interests may suffer. On these issues we need to have a more vigorous dialogue so that each side understands the rationale for the other's policy and the problems which may result from different corporate and government strategies. I hope and believe that these differences can be minimized so that when we are faced with an actual incident we will be working together rather than at cross-purposes.

International Cooperation. The final aspect of our strategy for dealing with terrorism and its proliferation is international cooperation. Here too we have made progress, although not as much as we would have liked. On a number of fronts the international community has demonstrated that it agrees with us that there are certain kinds of terrorist acts which are inadmissible in civilized society and which are contrary to the basic principles of international law. These include aircraft hijacking and sabotage, attacks on diplomats, and the taking of hostages. All of these acts are now covered by international conventions drawn up in the 1970s. The most recent is the Convention Against the Taking of Hostages which was opened for signature last December and which the United States signed almost immediately thereafter. This convention is before the Senate for ratification.

All of the conventions impose upon states party to them the obligation either to prosecute or extradite the perpetrators of these crimes. Unfortunately, not all crimes are covered by conventions—assassinations, bombings, and vessel hijackings are still outside this system of universal condemnation. In addition, none of the conventions provides for enforcement measures against states which violate their obligations as Iran did so flagrantly in the seizure of American hostages last November. The only exception is the undertaking of

copy for SS

seven leading aviation nations to cut off air services to countries which harbor hijackers. The Bonn declaration, as it is known, marks a significant turning point in international attitudes. We hope it will be extended to other areas, but we are realistic enough to realize that this process may take time and that some states will refuse to accept the limitations on their sovereignty which any system of sanctions implies.

As we look ahead to the last two decades of this century, we will undoubtedly see high levels of violence and turmoil. Increasing population pressures, growing competition for scarce resources, and widening income disparities within and between societies will create uncertainty and lead to various forms of conflict. Some of the turbulence in the world will take the form of traditional terrorism—hostage taking, kidnapping. Some will be in the form of urban unrest, revolution, and civil war. We must also anticipate continuing incidents of state-supported violence and terrorism. This phenomenon of state violence exercised through surrogate groups may, in fact, become one of the major political issues of the 1980s.

Nonetheless, high though the levels of violence may be, we need not despair. Government and the private sector have coped with violence in the past and can do so in the future. However, if we are to succeed, we will have to refine the tools which we have already identified—intelligence, security, crisis management, contingency planning, international cooperation.

Above all else, we must develop sound working relationships between government and industry. A close partnership is essential. Of especial importance will be research and development into techniques which will deter terrorists, protect executives, and deflect threats. One area which is already of great importance is the technological frontier represented by explosive taggants. Within the next decade we will be able to add to explosive materials both detection and identification taggants permitting us to spot bombs before they go off and to track down the perpetrators afterwards. This technology is of particular significance given the fact that bombs still represent the most numerous and most serious threat that we face. I have no reason to suppose that that situation will change in the years ahead.

If we are to cooperate more effectively, as I believe we must, we have to understand each other better and know where and how to get the information we need. This convention is enormously valuable in bringing together so many professional security experts for a detailed exchange of views, information, and technology. The American Society for Industrial Security makes a unique contribution to this process through its terrorism committee and its regional seminars.

In Washington, there is unfortunately no central point for information or assistance. However, I would like to commend to you a small pamphlet which the Department of Commerce has recently put out entitled "Combatting Terrorism: Sources of Federal Assistance for Business." It describes a number of places you can go for assistance and the kinds of help which are available. I know I speak for my colleagues at State, Commerce, the FBI, FAA, and Defense in saying that one of our principal responsibilities is to support and collaborate with the private sector. We need to know your concerns and your problems. We welcome the contact which meetings such as this provide. For they are sure signs of that spirit of partnership through which we can jointly meet the challenges of terrorism and low-level conflict in the 1980s.■

Published by the United States Department of State • Bureau of Public Affairs • Office of Public Communication • Editorial Division • Washington, D. C. • October 1980 • Editor: Norman Howard • This material is in the public domain and may be reproduced without permission; citation of this source would be appreciated.

Bureau of Public Affairs
United States Department of State
Washington, D.C. 20520

Official Business

If address is incorrect
please indicate change.
Do not cover or destroy
this address label ►

Postage and Fees Paid
Department of State
STA-501

Third Class Bulk Rate

U.S.MAIL

best copy available

READEX FICHE